AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Rosalinda Estrada-Dallis, a Special Agent (SA) with the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE), Kansas City, Missouri, being first duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the entire premises located at **8225 NW 82nd Ct, Kansas City, MO 64152 (TARGET PREMISES),** more particularly described in Attachment A1, and the person of JEFFREY KNIGHT, as described in Attachment A2, and to seize items relating to violations of 18 USC 2252, as more particularly described in Attachment B, as contraband, instrumentalities, and evidence of crime.

2. As a SA, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. At all times throughout this affidavit, I use the terms "child pornography" and "child sexual abuse material ("CSAM") merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction," "minor," and "sexually explicit conduct" as those terms are defined in 18 U.S.C. § 2252.

3. I am a Special Agent (SA) with the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE), currently assigned to Homeland Security Investigations (HSI), Kansas City, Missouri, and have been a SA since 2006. I have attended and successfully completed the Criminal Investigator Training Program (CITP) and the Immigration and Customs Enforcement Special Agent Training (ISAT) located at the Federal

Law Enforcement Training Center (FLETC) in Glynco, GA. Prior to becoming a SA, I was employed briefly as an Immigration Enforcement Agent (IEA) in Chicago, IL after being employed as a United States Customs and Border Protection Officer at O'Hare International Airport in Chicago, IL for approximately three (3) years. I received CBP training at the FLETC in Glynco, GA. As an HSI SA assigned to a Cyber Crimes group, I have investigated criminal violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18 United States Code 2251 and 2252. I have participated in the execution of numerous search warrants involving child exploitation and/or child pornography offenses and have participated in numerous investigations relating to the sexual exploitation of children. I have also observed and reviewed numerous examples of child pornography (as defined in Title 18 United States Code 2256) in various forms of media including computer media. I have discussed and reviewed these materials with other agents and other law enforcement personnel and have received formal basic training and instruction from experts in child pornography at the Immigration and Customs Enforcement (ICE) Special Agent Training Academy. As a federal agent, I am authorized to investigate violations of laws of the United States of America, and I am a law enforcement officer with the authority to execute warrants under the authority of the United States.

4. This affidavit is based upon information I have gained from my investigation, my training and experience, as well as upon information obtained from the Western Missouri Cyber Crimes Task Force (WMCCTF), and conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the

facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252 are located at the above address. Based upon the following information, there is probable cause to believe that currently located within the above-described premises is the evidence, fruits, and instrumentalities of trafficking, receipt, distribution, and/or possession of visual depictions, and other related materials, involving minors engaging in sexually explicit conduct (child pornography), as defined in Title 18, United States Code, Section 2256, and set out more fully in paragraph 27 below.

Background information

5. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

6. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal

identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number.)

7. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

8. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

9. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints

from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

10. NCMEC was established in 1984 as a private, nonprofit organization. NCMEC provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional authorization, NCMEC operates the Cyber Tipline, a forum for private citizens and businesses to report information related to the mission of the NCMEC, including the sexual exploitation of children. When NCMEC receives a Cyber Tipline report related to the sexual exploitation of children, they conduct some preliminary research to determine the location of the incident, and then forward the information to the appropriate ICAC task force or the appropriate law enforcement agency for follow-up.

11. In accordance with 18 U.S.C. § 2258A, if an Internet company such as Dropbox, Google, and Yahoo locates the presence of child pornography in a user's account, they will prepare a Cyber Tipline report to NCMEC. While Internet companies will report the presence of any child pornography, they find to NCMEC, they do not conduct an exhaustive search of a user's email account or cloud storage, but typically use some automated method for locating images of suspected child pornography.

12. NCMEC analysts are trained to analyze the information that is reported to them by Internet companies. The analysts can identify the ISP from the IP number. The geographical location in which a person's computer connects to the ISP's network is called the Point of Presence (hereafter referred to as PoP). Generally, IP numbers are mapped to PoP's or a geographic area.

By analyzing the IP, analysts can often determine the geographical location of the PoP that was accessed at the time the user was online and sent the offending content.

13. When a NCMEC analyst determines the probable geographical location of a PoP, he or she will route the CyberTipline information to the ICAC nearest to the PoP.

14. From my training and experience, I know that any computer that accesses the Internet must do so through an ISP. The ISP identifies the computer during the connection session by assigning it a unique number, called an IP address. This number is attached to all messages that come to and go from the computer.

PROBABLE CAUSE

15. In October 2021, the Western Missouri Cyber Crimes Task Force (WMCCTF) in conjunction with Homeland Security Investigations (HSI) Kansas City initiated an investigation as a result of numerous Cyber Tips (CT) received from the National Center for Missing and Exploited Children (NCMEC). The Cyber Tips (CT) reported a subject utilizing several platforms, including Dropbox and Google, to upload child pornography. The subject is associated to the following individual and e-mail addresses:

> Jeffrey KNIGHT / AKA: Jeff Knight
> Date of Birth: 08/08/1991
> Telephone: 813-295-4268
> E-mail addresses: (1) **jknight109291@gmail.com,** (2) **hollywoodfejj@yahoo.com** and (3) **jknight1092@gmail.com**, (4) **jknight1092@yahoo.com, (5) jefftheknight1092@gmail.com**

16. In total, the thirteen (13) CT Reports were associated to one of the three aforementioned e-mail accounts and reported uploads of suspected child pornography between

the dates of June 2014 and November 2021. The CT reports concerned a total of approximately eight hundred and seventy (870) files containing CSAM being uploaded by the aforementioned accounts. Several representative CT Reports are described below.

17. CT report 101674148 was reported by Dropbox to NCMEC in September 2021 and was associated to e-mail **jknight1092@gmail.com.** The CT Report covered file uploads occurring over a large period of time, with the earliest occurring December 2013 and the latest occurring in August 2017. Examples of the files include:

- One video file titled: **jason7.mp4,** depicts a pre-pubescent male fondling himself over his underwear and then removing his underwear and exposing his penis to the camera. Later in the video an adult male appears and begins fondling the child and performing oral sex on the child and vice versa. The file is approximately 42 minutes long. (Uploaded on 08/13/2017 at 13:31)

- One video file titled: **brccam S03E311 – The Omegle Game – 10yo Jesse and 8yo Duco.mp4,** depicts two (2) pre-pubescent males in a bed engaging in sexual activity, such as stroking their penis, stroking each other's penis, performing oral sex on each other, and thrusting as if they were having sexual intercourse. Throughout the video, the young males repeatedly look at the device recording them as if they are being instructed on what to do. The video is approximately 52 minutes long. (Uploaded on 11/14/2016 at 23:12)

- On video titled: **I_love.mp4,** depicts a pre-pubescent nude male and an adult male fondling each other, kissing, performing oral sex on one another and engaging in sexual intercourse. The video is 9 minutes and 35 seconds long. Uploaded on 01/20/2017 at 08:13)

18. CT Reports 103830787, 106025449, and 106039246, were reported by Google, Inc., to NCMEC in October 2021. These CT Reports were associated with e-mail account **jknight109291@gmail.com**. The following are examples of the files uploaded to Google by the e-mail account.

- One file titled: **report_15004137645570091830. Jpg or IMG_0229.JPG,** depicts a boy of approximately 13-15 years of age, looking up at the camera with an adult

penis in his mouth. (Uploaded on 10/02/2021 at 07:33:53 UTC)

- One file titled: **report_7590034240551230409.jpg or IMG_0172.JPG** depicts an image of (4) four nude boys between the ages of approximately 10-13 years of age, sitting on a couch. (Uploaded on 10/02/2021 at 07:33:38 UTC)

- On file titled: **report 7293153913788966420.jpg or IMG_0180.JPG** depicts a nude boy of approximately 14-16 years of age, sitting with his legs spread apart in the air while inserting a white object into his anus. (Uploaded on 10/02/2021 at 07:33:38 UTC)

- One file titled: **report_10239811719280891285 or IMG_0213.JPG**, depicts a screen shot of an image taken from a gallery depicting a pre-pubescent nude boy sitting on the lap of a nude adult male with an erect penis. The screenshot appears to have been taken on a cellular device because the image also shows a battery icon and wi-fi icon at the top of the image. (Uploaded on 10/02/2021 at 07:33:44 UTC)

- One file titled: **report_6877951122091039314 or IMG_0201.JPG,** depicts a screenshot of a pre-pubescent child bending over with their bottoms pulled down exposing their buttocks. The top of the image shows the time and battery meter icon. (Uploaded on 10/02/2021 at 07:33:43 UTC)

19. The CT Reports for the last two images provided Internet Protocol (IP) address information for the IP address used to upload files **report_10239811719280891285 or IMG_0213.JPG and report_6877951122091039314 or IMG_0201.JPG** to Google by jknight109291@gmail.com. The IP address **2601:300:4500:1870:206d:eb5d:f587:2df5** was used to upload these files. Affiant conducted an open source internet query of IP address: **2601:300:4500:1870:206d:eb5d:f587:2df5** and discovered the IP address resolved to Internet Service Provider (ISP) Comcast.

20. On February 16, 2022, a summons was sent to Comcast requesting information pertaining to IP address: **2601:300:4500:1870:206d:eb5d:f587:2df5** from October 2,2021 at 07:33:32 UTC through October 2, 2021, at 07:40:52 UTC. Comcast responded on March 30, 2022, with the following account information assigned on October 2, 2021, at 07:33:32 UTC. :

Subscriber Name: Jeffrey **KNIGHT**
Service Address: 725 SW 29th Street
Blue Springs, MO 64015-3364
Telephone: (813) 295-4268
Account number: 8512100050615881
Start of service: 2/15/2020
Account status: Disconnected 10/28/2021
E-mail user IDs: jknight1092

21. CT report 103417835 was reported to NCMEC by Google in October 2021 as well and was associated with email addresses **jknight1092@gmail.com** and **Hollywoodfejj@yahoo.com.** NCMEC reported that five (5) of the suspected CSAM files located within this CT Report appeared "unfamiliar", which indicates those files may have been newly produced.[1] These files were stored within the Google infrastructure and had been uploaded using the associated email address in February 2020.

a. One of the files, titled: **report_12076142216785095434** or **IMG_0150.HEIC** depicts a clothed child holding what appears to be an adult male's penis. Only the child's hand and clothed lower body is visible in the image. This file was uploaded on 02/03/2020 at 11:59:09 UTC. Google provided EXIF[2] data for this file, which included the following information:

- EXIF camera make: Apple
- EXIF camera model: Iphone 11 Pro Max
- EXIF date created: 2020:02:02 19:40:04
- EXIF latitude 39.011344444444447
- EXIF longitude -94.297363888888881

b. Another file in CT Report 103417835, titled **Google_CT RPT-93268ddd770c30c52006cb794f134aca-IMG_0149.MOV or IMG_0149.MOV** depicts a boy of

[1] By way of explanation, "familiar" files are those previously known to NCMEC through other investigations, and can be identified by a known victim, hash value, or other identifying information.
[2] **EXIF** (Exchangeable Image File Format) is a standard that defines specific information related to an image or other media captured by a digital camera. It is capable of storing important data such as camera exposure, date/time the image was captured, and even GPS location.

approximately 4-6 years of age, with his pants pulled down, laying on his back, while an adult male fondles and performs oral sex on him. The video is 10 seconds long. The child in this video appears to be the same child seen in the file mentioned in the preceding paragraph, and the video appears to have been taken in the same room. This video was uploaded on 02/03/2020 at 11:59:35 UTC.

c. A third file, titled**: Google-CT-RPT-6b30c2d10af8d24edc2f7adc476881ad-IMG_0147 or IMG_0147.MOV**, depicts a child's hand stroking an adult male's penis. This file appears to involve the same child in the preceding paragraphs and appears to have been taken at or near the same time as the previous videos as the child is wearing the same clothing. This video was uploaded on 02/03/2020 at 11:59:46 UTC.

22. An open-source search of the EXIF GPS coordinates utilizing Google Maps, shows coordinates resolve to 808 SW 29th Street, Blue Springs. This address is located four houses down and across the street from, 725 SW 29th Street, Blue Springs, Missouri, the address associated to JEFFREY KNIGHT and the physical location of the IP address associated with the previously discussed CT Reports.

23. On September 1, 2022, a summons was sent to Google requesting subscriber information for jknight1092@gmail.com and Google provided the following the next day:

Name: Jeff Knight
Created on: 04/18/2011
End of service date: 09/30/2021
Recovery e-mail: Hollywoodfejj@yahoo.com
Recovery SMS: 813-295-4268

24. On September 1, 2022, another summons was sent to Google requesting subscriber information for e-mail address: jknight109291@gmail.com and Google responded with the following the next day:

Google Account ID: 671702758135
Name Jeffrey Knight
Created on: 09/30/2021
End of service date: 10/04/2021
Recovery SMS: 813-295-4268

25. On March 14, 2022, another summons was sent to Yahoo requesting subscriber information pertaining to e-mail account: holllywoodfejj@yahoo.com and Yahoo responded with the following on March 17, 2022:

Account status: active
Registration IP address: 24.73.152.228
Registration date: 09/05/2004
Full name: Jeff KNIGHT
City: Oveido
State: FL
Recovery e-mails: eltontonnn@gmail.com
Recovery phones: 813-295-4268

26. In an attempt to obtain more current information on login activity and to determine whether this account was still active, another summons was sent to Yahoo on September 1, 2022, and a response was received on September 2, 2022. A review of the return discovered the account was still active and there had been some updates on the account. The recovery e-mail address had been updated to **jknight1092@yahoo.com** and recovery phone was updated to **(816) 788-4088**, all of which are associated to Jeffrey Knight.

27. Open-source research revealed that phone number (813) 295-4268, associated with the Comcast, Google, and Yahoo accounts listed above, was assigned to Verizon Wireless. On February 16, 2022, a summons was sent to Verizon Wireless requesting subscriber information for this number, and they responded in the same month, with the following:

Account number: 525880268-1
First name: Anthony
Last name: Cuervo

Address: 1322 Gangplank Drive, Valrico, FL 33594
Contact Last name: KNIGHT
Contact First name: Jeffrey
Effective date: 09/25/2020
Disconnect date: 4/23/2021

28. Based on the disconnect date of (813) 295-4268 and the updated information in the Yahoo account, law enforcement conducted additional searches to determine KNIGHT's current phone number. Law enforcement searches revealed the number (816) 788-4088 was associated with KNIGHT. An open-source search found that the phone number resolved to T-Mobile. On September 7, 2022, a summons was sent to T-Mobile requesting subscriber information and T-Mobile responded with the following:

Customer name: Jeff Knight
Subscriber name: Jeff Reyknight
Service/Billing Address: 8225 NW 82nd Ct, Kansas City, MO 64152
Service Start Date: June 24, 2022
Service is currently active as of January 6, 2023.

29. In July 2022, HSI Kansas City received information from the United States Postal Inspection Service (USPIS) that KNIGHT moved from 725 SW 29th Street, Blue Springs, Missouri to 8225 NW 82nd Ct, Kansas City, Missouri. As of January 13, 2023, the USPIS confirmed KNIGHT, and J Knight Transport, LLC. currently receive mail at 8225 NW 82nd Ct, Kansas City, MO, 64152.

30. On July 22, 2022, HSI agents conducted surveillance at **TARGET PREMISES** and observed a male entering a white tractor trailer that was parked in the driveway of the home. Agents observed the tractor trailer had the following markings: RTA Logistics Inc., DOT: 3159384 and MC 110361. While conducting surveillance, agents observed a white male enter the tractor trailer and drive to the Oak Grove 70 Trucker stop to pick-up a trailer and then drove

to T Force Freight in Kansas City, Kansas.

31. HSI Kansas City agents thereafter requested the assistance of the Department of Transportation-Office of Inspector General (DOT-OIG) in an effort to obtain further information on the driver of the tractor trailer. DOT-OIG database checks discovered Jeffrey Allen Knight, DOB: 08/08/1991, MO license 112C006005, and mailing address: 725 SW 29th Street, Blue Springs, MO was a driver for RTA Logistics Inc., located in Woodridge, Illinois.

32. On September 21, 2022, agents again conducted surveillance at **TARGET PREMISES** and observed a white male, believed to be KNIGHT, exit the residence with a backpack and duffel bag. The white male placed the duffel bags in the bobtail truck and stayed inside the truck for a few minutes before exiting and going back into the residence. The bobtail truck had the following markings: "Cargorunner.com". The white male was observed departing the residence in the truck a few minutes later. It is known to agents that KNIGHT has been a truck driver for several years and recently filed an application for Articles of Organization, in the state of Missouri, for a limited liability company by the name of JKnight Transport LLC.

33. On October 11, 2022, HSI Kansas City was contacted by the Western Missouri Cyber Crimes Taskforce (WMCCTF) regarding six (6) additional Cyber Tip Reports they had received related to Jeffrey KNIGHT and e-mail addresses: **jeffthеknight1092@gmail.com** and **jknight1092@yahoo.com**. These reports were submitted to NCMEC by Google in August 2022 and reported uploads of suspected CSAM to Google by the associated e-mail addresses between approximately March 7, 2022, and May 12, 2022. A total of approximately 392 files containing CSAM were reported in these six (6) CT reports. The following are examples of the files:

- One file titled: **IMG_0101.JPG**, depicts a nude pubescent male under the age of 18, laying on a bed with an erect penis. (CT # 130912927, uploaded on

03/07/2022 at 01:38:56 UTC)

- One file titled: **d804963369f94fcab7a70e7178c614ae.mov**, depicts a pre-pubescent boy masturbating. (CT # 130912927, uploaded on 05/02/2022 at 04:10:05 UTC)

- One file titled: **VID-20150111-WA0033.mp4**, depicts a video of a fully clothed pre-pubescent boy who later pulls down his pants and exposes himself and masturbates directly at the camera. The boy appears to be typing and looking at a monitor during the video. (CT# 130898887, uploaded on 04/10/2022 at 00:52:24 UTC)

- Another file titled: **IMG_201.JPG**, depicts a screenshot of a pre-pubescent child bending over with their bottoms pulled down exposing their buttocks. The top of the image shows the time and battery meter icon. (CT# 130707946, uploaded on 04/07/2022 at 05:50:14 UTC) This file is the same image of the possibly produced CSAM discussed above that was reported by Google in October 2021 in CT# 106039246 and associated to email address: **jknight109291@gmail.com.**

34. On October 14, 2022, a summons was sent to Google requesting subscriber information pertaining to newly discovered email account **Jefftheknight1092@gmail.com**. Google responded with the following on the same day:

> Name: Jeffrey Knight
> Created on: 2022-02-27 17:54:44 Z
> End of Service Date: 2022-08-12 06:20:19 Z
> Recovery e-Mail: jknight1092@yahoo.com
> Recovery SMS: +18167884088
> Address: 8225 NW 82nd CT, Kansas City, MO 64152

35. Google also provided IP login history for the Google account **Jefftheknight1092@gmail.com**. On June 11, 2022, the Google account logged in utilizing IP address **2605:a601:ae82:da00:a99f:ea17:77ac:117a**. On August 10, 2022, the Google account logged in using IP address **2607:fb90:d308:a97d:553d:247e:975e:7bc5.**

36. An open-source database search discovered IP address

2605:a601:ae82:da00:a99f:ea17:77ac:117a resolved to Google Fiber. In October 2022, a summons was sent to Google Fiber requesting subscriber information for this IP address and Google responded with the following:

> Primary contact User profile
> Name: Jeff Knight
> Primary e-mail: knighttransport03@gmail.com
> Mobile phone: 8167884088
> Street address: 8225 NW 82nd Ct, Kansas City, MO 64152-4628

37. An open-source database search discovered IP address **2607:fb90:d308:a97d:553d:247e:975e:7bc5** resolved to T-Mobile. In October 2022, a summons was sent to T-Mobile requesting subscriber information for various IP addresses including **2607:fb90:d308:a97d:553d:247e:975e:7bc5** and T-Mobile responded with the following:

> Subscriber/ Account name: Jeff Reyknight
> Subscriber address: 8225 NW 82nd Ct, Kansas City, MO 64152
> Begin service date: 06/24/2022
> MSISDN: 816-788-4088
> IMEI: 35379435452027
> Billing details
> Bill name: Jeff Reyknight
> Bill Birth Date: 08/08/1991
> Bill SSN: 486-08-8441
> Bill address: 8225 NW 82nd Ct., Kansas City, MO 64152
> Contact name: 816-788-4088

38. In January 2023, information received from local law enforcement found that the water service at 8225 NW 82nd Ct, Kansas City, Missouri is registered to JEFFREY KNIGHT.

39. HSI agents conducted a drive-by of **TARGET PREMISES** and made the following observations: the residence is a two-story, single-family home composed of aluminum

siding. The home is painted gray and has white trim. The numbers "**8225**" are clearly marked in black on the trim, on the left- hand side of the 2-car garage door. The residence sits on a corner lot, on the corner of Conant Ave. and 82nd Ct and faces east. The residence is located in Platte County, Kansas City, Missouri.

40. It is Affiant's opinion that JEFFREY KNIGHT, utilizing e-mail accounts **jknight109291@gmail.com, hollywoodfejj@yahoo.com**, **jknight1092@gmail.com**, and **jefftheknight1092@gmail.com**, on diverse occasions uploaded suspected CSAM to both Dropbox and Google accounts between December 2013 and May 12, 2022. All IP address information that has been discovered concerning those uploads has resolved, most recently, to JEFFREY KNIGHT'S prior residence at 725 SW 29th Street, Blue Springs, Missouri. Additionally, it appears that each of his known e-mail accounts, with the exception of jknight1092@yahoo.com and hollywoodfejj@yahoo.com have been closed prior to the date of this affidavit. It appears, in Affiant's opinion, that whenever an e-mail account of JEFFREY KNIGHT'S is closed, he creates a new one utilizing a similar naming convention, but with slight deviations in the characters. Finally, while IP address information is not available for uploads of CSAM directly from **TARGET PREMISES**, current evidence establishes that the e-mail account **jefftheknight1092@gmail.com**, associated with JEFFREY KNIGHT, and which had previously been associated with the uploading of CSAM to Google, was accessed at **TARGET PREMISES** prior to that e-mail account's closure on August 12, 2022, and has specifically been listed by JEFFREY KNIGHT as being associated with his current address.

41. In Affiant's experience, collectors of child pornography who view, possess, produce and/or share CSAM take pride in their collection and save the CSAM on electronic

devices and in their home for viewing and sharing at their leisure. People who like to view and share CSAM material do not knowingly leave their CSAM collection behind when they move from one residence to another. People interested in CSAM often view the child pornography surreptitiously and away from those closest to them, including spouses and significant others. It is Affiant's opinion that JEFFREY KNIGHT can be considered a collector of child pornography based on his long history of involvement with child pornography, coupled with the fact that even though his email accounts are closed for likely violating terms of service, he opens new accounts and continues to traffic in child pornography. Because he is also able to continue to traffic child pornography when an account is closed, it is likely that he has stored copies of the child pornography he traffics in locally on electronic devices that he can access without his specific internet account.

42. I am aware that a number of courts have found probable cause in cases involving persons involved in the possession and trafficking of child pornography where the subject moved to a new residence during the course of the investigation. *See, e.g., United States v. Epps*, 570 Fed. Appx. 197, 200 (3rd. Cir. 2014)(unpublished)("magistrate reasonably could have inferred that [the defendant] would take the computer with him or otherwise transfer the digital collection of child pornography when he moved to his new residence less than a year prior to the search . . . we have never required the government to prove that a computer used for uploading child pornography in a former residence was actually moved to a new residence before authorizing a search of the new residence."); *United States v. Richardson*, 670 F.3d 357 (4th Cir. 2010); *State v. Felix*, 942 So.2d 5 (Fla. 2006);); *State v. Ingold*, 2008 WL 2026441 (Ohio May 13, 2008)(unpublished); *United States v. Hudson*, 2020 WL 8083659 (D. Minn. Dec. 19,

2020)(unpublished).

DEFINITIONS

43. Title 18, United States Code, Section 2256, et. seq. defines, for the purposes of Section 2252, the following terms:

(1) "Minor" means any person under the age of eighteen (18) years;

(2) "Sexually Explicit Conduct" means actual or simulated-

a) sexual intercourse, including genital- genital, oral-genital, anal-genital, or oral- anal, whether between persons of the same or opposite sex;

b) bestiality;

c) masturbation;

d) sadistic or masochistic abuse; or

e) lascivious exhibition of the genitals or pubic area of any person.

(3) "Producing" means producing, directing, manufacturing, issuing, publishing, or advertising.

(4) "Visual Depiction" includes undeveloped film and video tape, data stored on a computer disk or by other electronic means which is capable of a conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

(5) "Computer" is defined pursuant to Title 18 United States Code, Section 1030(e)(1), as: an electronic, magnetic, optical, electrochemical, or other

high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator, or other

similar device.

44. "Child Erotica," as used herein, means materials demonstrating a sexual interest in minors, including fantasy narratives, cartoons and books describing or alluding to sexual activity with minors, sexual aids, children's clothing catalogues, and child modeling images.

45. I know that computer hardware and computer software may be utilized to store records which include, but are not limited to, those related to business activities, criminal activities, associate names and addresses, and the identity and location of assets illegally gained through criminal activity.

46. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

a. Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements, receipts, returns, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets.

b. Graphic records or representations, photographs, slides,

drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes, and aural records or representations, tapes, records, disks.

47. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications that may have been created or stored, including (but not limited to): any hand-made form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); and any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, smart phones, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

48. I am familiar with the following facts based upon my own personal observations, as well as information officially supplied to me by other law enforcement agents and/or officers.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

49. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other.

50. The development of computers and smart phones has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are: production, communication, distribution, and storage.

51. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, smart phone, or mobile device, so that the image file is stored in his computer, phone, or mobile device.

52. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been

viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

53. The computer's capability to store images in digital form makes it an ideal repository for pornography. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera or camera on a phone to capture an image, process that image in a computer with a video capture board, and to save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

54. Smart phone technology has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, and store and view movie and picture files.

The Internet and Definitions of Technical Terms Pertaining to Computers

55. As part of my training, I have become familiar with the Internet (also commonly

known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit websites (see definition of "websites" below) and make purchases from them.

56. Set forth below are some definitions of technical terms, used throughout this Affidavit pertaining to the Internet and computers more generally.

a. **Computer system and related peripherals, and computer media**: As used in this affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer- related operation equipment, digital cameras, scanners, smart phones, mobile devices in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats,

including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

b. **Internet Service Providers (ISPs) and the Storage of ISP Records**: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and personal password. ISPs maintain records ("**ISP records**") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "**electronic storage**," see 18 U.S.C.
§ 2510(17), and the provider of such a service is an "**electronic communications service**." An "**electronic communications service**," as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "**remote computing service**." 18 U.S.C. § 2711(2).

c. **Internet Protocol Address (IP Address):** Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every

telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISPs employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISPs, including most cable providers, employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each, and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

d. **Log File**: Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log on/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

e. **Website**: A website consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

f. **Website Hosting**: Website hosting provides the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a server and perhaps a web hosting company to host it. "**Dedicated hosting**" means that the web hosting company provides all of the equipment and assumes

all the responsibility for technical support and maintenance of a website. "**Co-location**" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically
house their hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEM

56. Based upon your Affiant's knowledge, training, and experience, and the experience of other law enforcement personnel, your Affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or laboratory. This is true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crimes related to violations of Title 18 U.S.C. Sections 2252 and 2256. Data unrelated to those violations will not be saved or copied. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely

vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

57. Based upon your Affiant's consultation with experts in computer searches, data retrieval from computers, and related media and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your Affiant knows that searching computerized information for evidence or instrumentalities of crime commonly require agents to seize all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them in a reasonable time.

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as central processing unit (CPU). In cases like this one where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. In addition, there is probable cause to believe that the computer and its storage

devices, the monitor, keyboard, and modem are all instrumentalities of the crime of transmitting child pornography in violation of law and should all be seized as such.

d. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the **TARGET PREMISES** are protected materials pursuant to the PPA.

If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

CONDUCT OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY

58. Pursuant to my training and experience, as well as the training and experience of other law enforcement personnel, I have learned that:

a. Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contact with other individuals who have it available.

b. The use of computers to traffic in, trade, or collect child pornography and obscenity has become one of the preferred methods of obtaining obscene and child pornographic materials. An individual familiar with a computer can use it, usually in the privacy of his own home or office, to interact with another individual or a business offering such materials in this country or elsewhere in the world. The use of a computer provides individuals interested in obscenity or child pornography with a sense of privacy and secrecy not attainable by other media. It also permits the individuals to contact and interact with many more individuals than through the use of the mails.

c. Your Affiant is aware from training and experience that persons involved in sending or receiving child pornography tend to retain it for long periods of time. This includes retaining the electronic media which the child pornography is stored on. Further, when collectors of child pornography obtain new electronic media, they tend to copy their child pornography collections onto this new electronic media. This tendency to retain these child pornography collections is enhanced by the increased sense of security that a computer affords. In addition, your Affiant is aware from training and guidance that persons who procure child pornography and who have a proclivity for sexual activity involving youths, obtain and retain magazines, films, videos, pictures and other items of child pornography as well as correspondence, advertising, bills, and notes relating to sexual activity involving children for long periods of time and do not dispose of or destroy such materials except to trade

such materials with others in exchange for similar items. **In addition, your Affiant's training has shown that such material is normally and generally kept in the individual's residence or other secure location to ensure convenient and ready access. I am also aware through my training and experience that collectors of child pornography tend to bring their child pornography collections, and the electronic media it is stored on, with them when they move from one residence to another, as they tend to always want it to be in a secure, private location near them.**

CONCLUSION

59. Based upon the foregoing, your Affiant asserts that probable cause exists that the computer, computer media, and related documents pertaining to the acquisition, and distribution of child pornography, are located on the premises at **8225 NW 82nd Ct, Kansas City, MO 64152** and on the person of **JEFFREY KNIGHT.**

60. Your Affiant would respectfully suggest there is probable cause to believe these records are maintained in files, computer storage facilities or other data storage facilities, and that, within these files, there are records--namely, correspondence, notes, papers, ledgers, personal telephone and address books, telephone toll records, telephone message slips, memoranda, telexes, facsimiles, documents, photographs, negatives, photographic slides or other visual depictions or equipment--used to depict child pornography materials.

61. Additionally, your Affiant believes that evidence of violations of 18 U.S.C. § 2252 are contained or concealed in CD Rom disks, DVD disks, thumb drives, video tapes, computer tapes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk applications programs, data disks, system disk operating systems, magnetic media- floppy disks, tape systems and hard drive, smart phone or mobile device, and other computer related

operating equipment, which depict or are used to depict child pornographic materials contrary to the laws of the United States.

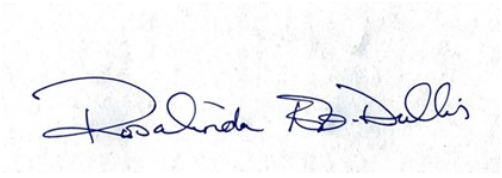
62. Based on all the foregoing, your Affiant respectfully suggests there is probable cause to believe that child pornography, and other evidence of the use of computers to traffic in child pornography, as set forth in the attached search warrant, will be found on the premises located at **8225 NW 82nd Ct., Kansas City, MO 64152** and under the control of **JEFFREY KNIGHT** and/or other individuals unknown, as well as on the person of **JEFFREY KNIGHT** and those items of child pornography constitute merchandise imported distributed and/or transported across state lines contrary to the laws of the United States.

63. Your Affiant respectfully requests that a search warrant be issued authorizing the Homeland Security Investigations, with the appropriate assistance from other law enforcement officers, to search for and to seize items listed in the attached Attachment B, which is property that constitutes evidence of a criminal offense in violation of 18 U.S.C. § 2252 and also contraband, the fruits of a crime, or things otherwise criminally possessed.

Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that an individual, specifically JEFFREY KNIGHT, possesses child pornography in violation of 18 U.S.C. § 2252. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. § 2252 may be found in JEFFREY KNIGHT'S current residence, listed in Attachment A1 , and on the person of JEFFREY KNIGHT, listed in Attachment A2 to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property

which is or has been used as the means of committing the foregoing offenses.

FURTHER AFFIANT SAYETH NOT.



Rosalinda Estrada-Dallis, Special Agent
Homeland Security Investigations

Sworn and subscribed to me by telephone on this 30th day of January 2023.

At 1:19 pm

HONORABLE W. BRIAN GADDY
United States Magistrate Judge
Western District of Missouri